山西大学学报(自然科学版)48(2):381—390,2025
Journal of Shanxi University(Nat. Sci. Ed.)

DOI:10.13451/j.sxu.ns.2024146

大数据环境下隐私保护边缘计算架构的研究

马海昕[1*],白鹤翔[2]
(1.山西财贸职业技术学院,山西 太原 030031;
2.山西大学 计算机与信息技术学院,山西 太原 030006)

摘 要:随着信息技术的迅猛发展,大数据时代已全面到来。边缘计算通过将计算和存储资源部署在网络边缘,逐渐成为解决数据处理瓶颈的关键技术。然而,现有边缘计算方案在隐私保护方面仍存在用户管理机制缺失、底层密码原语依赖和适用场景固化等问题。为解决这些挑战,本文提出了一种新型隐私保护边缘计算架构,结合了区块链审计机制和可自定义的密码原语特性。该架构通过引入区块链技术加强用户管理和防范恶意行为,同时允许底层密码原语的自定义,以适应多种应用场景。文章以Paillier密码系统为例,详细描述了架构的设计和工作流程,并提供了形式化的安全证明。此外,本文对新架构进行了性能分析,通过在三种数据集上对Paillier、ElGamal和CKKS加密算法进行仿真测试。结果表明,本文设计的新隐私保护边缘计算架构符合多场景的工业应用标准,且具有较高的实用性和安全性。

关键词:同态加密;CKKS;云计算;Paillier;区块链
中图分类号:TP309 **文献标志码**:A **文章编号**:0253-2395(2025)02-0381-10

Privacy-preserving Edge Computing Architecture in Big Data Environment

MA Haixin[1*], BAI Hexiang[2]
(1. *Shanxi Vocational and Technical College of Finance and Trade, Taiyuan* 030031*, China;*
2. *School of Computer and Information Technology, Shanxi University, Taiyuan* 030006*, China*)

Abstract: With the rapid development of information technology, the era of big data has fully arrived. By deploying computing and storage resources at the edge of the network, edge computing has gradually emerged as a key technology to address data processing bottlenecks. However, existing edge computing schemes still suffer from some issues in terms of privacy protection, such as lack of user management mechanisms, dependency of underlying cryptographic primitives, and solidification of applicable scenarios. To address these challenges, this paper proposes a novel privacy-preserving edge computing architecture that combines blockchain auditing mechanisms with customizable cryptographic primitives. The architecture enhances user management and malicious behavior prevention through blockchain technology while allowing the customization of cryptographic primitives to accommodate various application scenarios. The paper uses the Paillier cryptosystem as an example to describe the architecture's design and workflow in detail, and provides a formal security proof. Additionally, the paper conducts a performance analysis of the new architecture by simulating Paillier, ElGamal, and CKKS encryption algorithms on three datasets. The results demonstrate that the proposed privacy-preserving edge computing architecture meets the industrial application standards for multiple scenarios and exhibits high practicality and security.

Key words: homomorphic encryption; CKKS; cloud computing; Paillier; blockchain

收稿日期:2024-09-05;**接受日期**:2024-10-24
基金项目:国家自然科学基金(41871286)
* **通信作者**:马海昕(1984—),男,山西太原人,硕士,讲师,研究方向为大数据、云计算、信息安全。E-mail:38369429@qq.com
引文格式:马海昕,白鹤翔.大数据环境下隐私保护边缘计算架构的研究[J].山西大学学报(自然科学版),2025,48(2):381-390. DOI:10.13451/j.sxu.ns.2024146.

0 引言

随着物联网[1]、5G(5th Generation Mobile Networks)[2]、AI(Artificial Intelligence)大模型[3]等前沿技术的快速发展,传统的集中式云计算架构在低延迟、高带宽需求和隐私保护等方面逐渐显露出无法满足现代应用需求的局限性。边缘计算[4-5]通过将计算资源和数据存储部署在靠近数据生成源(如传感器、移动设备、车载终端等)的网络边缘,而非依赖于远端的集中式数据中心,来改善系统性能和数据处理效率。这种新兴技术使数据处理更接近数据源,从而减少了数据传输的延迟,提高了响应速度,同时优化了带宽利用率。这种计算架构能够在设备本地或近旁处理数据,显著提升了实时性和处理效率,同时也增强了隐私保护,因为敏感数据可以在本地处理,而不必传输到远端数据中心。

边缘计算因其低延迟、低带宽消耗、高容错性和强大可扩展性等优势,能够满足海量数据计算的需求,吸引了众多学者的关注,并在这一领域取得了显著的突破。例如,Liu等[6]提出了一种基于区块链技术的移动边缘计算框架,该框架能够自适应地处理视频流块,从而提高视频传输的效率和质量。Pace等[7]设计了一种针对新兴医疗保健行业的边缘计算框架,该架构由微型移动客户端模块和边缘网关组成,能够高效地收集并本地处理来自不同场景的数据,提升了医疗数据处理的实时性。Nguyen等[8]则推出了一个名为BEdgeHealth的分布式医疗边缘计算架构,该架构结合了移动边缘计算与区块链技术,用于分布式医院网络中的数据卸载和共享。此外,边缘计算在各种应用场景中的架构设计也得到了广泛研究,例如节能应用场景[9]、车载终端边缘计算[10-11]以及人工智能场景[12-13]等。然而,这些研究虽然展示了边缘计算在各个应用场景中的可行性,却在很大程度上忽视了架构中的隐私保护问题。在处理和存储敏感数据时,如何有效保障数据的隐私性仍然是边缘计算领域面临的重大挑战。

为了使边缘计算架构能够同时满足数据处理和隐私保护的双重需求,学术界和工业界纷纷聚焦于隐私保护边缘计算的研究。Sheikhalishahi等[14]构建了一种保护边缘云数据安全的隐私保护边缘计算架构,该架构能够满足数据提供者的隐私需求,但需要在计算隐私性与结果准确性之间进行权衡。He等[15]则采用改进的Paillier加密算法作为底层加密技术,设计了一种低延迟的隐私保护边缘计算方案,以保护终端设备的隐私。Liu等[16]开发了一种隐私保护模型定制框架,该框架能够在不收集原始数据的情况下有效地定制从云到边缘设备的卷积神经网络(Convolutional Neural Network,CNN)模型。Jiang等[17]推出了一种结合混合差分隐私和自适应压缩的联邦边缘学习框架,该框架通过自适应差分隐私模型实现了对工业环境中梯度参数传输的隐私保护。与传统的边缘计算研究类似,学者们也将隐私保护边缘计算方案应用于多种场景中[18-21]。然而,现有的隐私保护边缘计算架构仍然面临一些挑战,例如用户管理机制的缺失和对底层密码原语的依赖等问题。这些挑战表明,在实际应用中,隐私保护边缘计算仍需进一步优化和完善。

为了解决上述问题,本文设计了一种用户管理机制完善、可自定义底层密码原语的可适用场景多类型应用场景的新隐私保护边缘计算架构,即基于区块链审计机制的用户自定义隐私保护边缘计算架构(User-defined privacy-preserving edge computing architecture based on blockchain audit mechanism, UPECA)。该架构既保障边缘数据的计算隐私性又实现了架构自适用性,其主要贡献点如下:

(1)首先,文章设计出一种适用于隐私保护边缘计算架构的区块链审计机制。该机制不仅增加了用户管理机制用于用户恶意行为防范,而且实现了底层密码原语的自定义功能,以确保架构适用于多类型应用场景。

(2)其次,文章的底层加密原语选取了Paillier密码系统作为样例,详细地描述了新架构的工作流程,并给出了形式化的安全证明。

(3)最后,文章给出了新隐私保护边缘计算架构的性能分析。新架构选取了Paillier加密算法、ElGamal加密算法和CKKS加密算法在三种数据集上进行了仿真模拟。分析结果表明本文设计的新隐私保护边缘计算架构符合多场景的

工业应用标准,且具有较高的实用性和安全性。

1 预备知识

1.1 边缘计算

边缘计算[4-5]是一种分布式计算模型,它将数据处理和存储位置从传统的集中式云数据中心向接近数据源的边缘设备或边缘节点推移,以便更快速地响应数据处理需求和降低网络传输延迟。这种新兴计算范式可以减少数据传输的延迟和带宽需求,提高数据处理的速度和效率,特别适用于需要实时响应和较低延迟的应用场景。如图1所示,边缘计算通常分为设备层、边缘节点层、边缘计算层、云平台层四个层次。

1.2 区块链审计机制

区块链审计机制[22-23]是指对区块链系统中的数据和交易进行审计和验证的方法和流程。由于区块链的去中心化特性和不可篡改的设计,审计机制在确保系统安全、可靠性和合规性方面至关重要。在本文中,区块链审计机制的设计目标是防范恶意用户的非法请求、增加用户管理机制和实现底层密码原语的自定义功能。如图2所示,隐私保护系统会涉及数据加密操作,密钥对(pk, sk)将上传至区块链维护的密钥管理表,计算终端间的计算结果也会写入区块链中,需各节点达成共识。

此外,计算终端间的运算结果也需要写入区块链。由于区块链的去中心化特性和不可篡

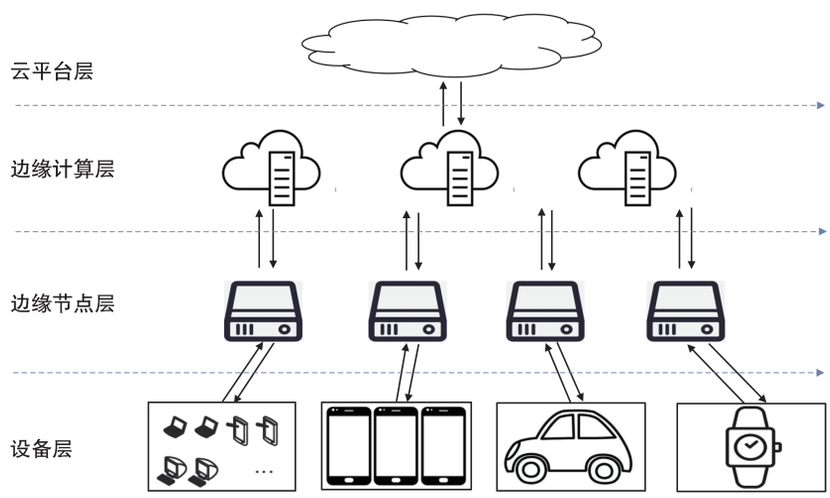


图1 边缘计算的网络模型

Fig. 1 Network model of edge computing

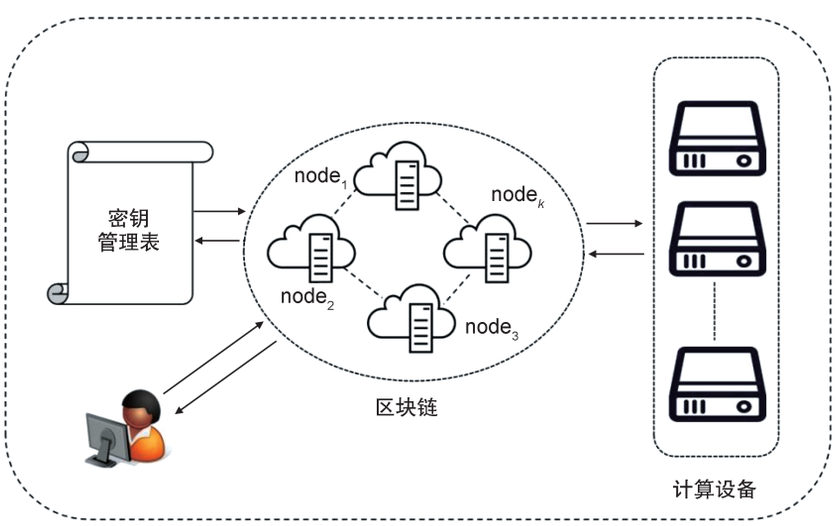


图2 区块链审计机制

Fig. 2 Blockchain-based audit mechanism

改的特性,所有操作数据都能在审计过程中还原。因此,区块链审计机制实现了防范恶意用户的非法请求和用户安全管理的机制。

2 模型介绍

2.1 系统模型

2.1.1 系统模型的介绍

新隐私保护边缘计算架构UPECA的系统模型如图3所示。涉及系统运行的实体有云平台、区块链节点、用户、边缘终端、密钥管理表。详细说明如下:

(1)云平台:云平台属于非权威第三方,用于全局密码(PK, SK, $f(x)$)生成,并通过Shamir秘密分割门限技术将SK分割为各子密码(PK, sk_i, $f(x_i)$),发送至各区块链节点。

(2)区块链节点:区块链节点获取子密码(PK, sk_i, $f(x_i)$)维护区块链运算。在需要审计操作时重构全局私钥SK,用于查询终端操作记录。

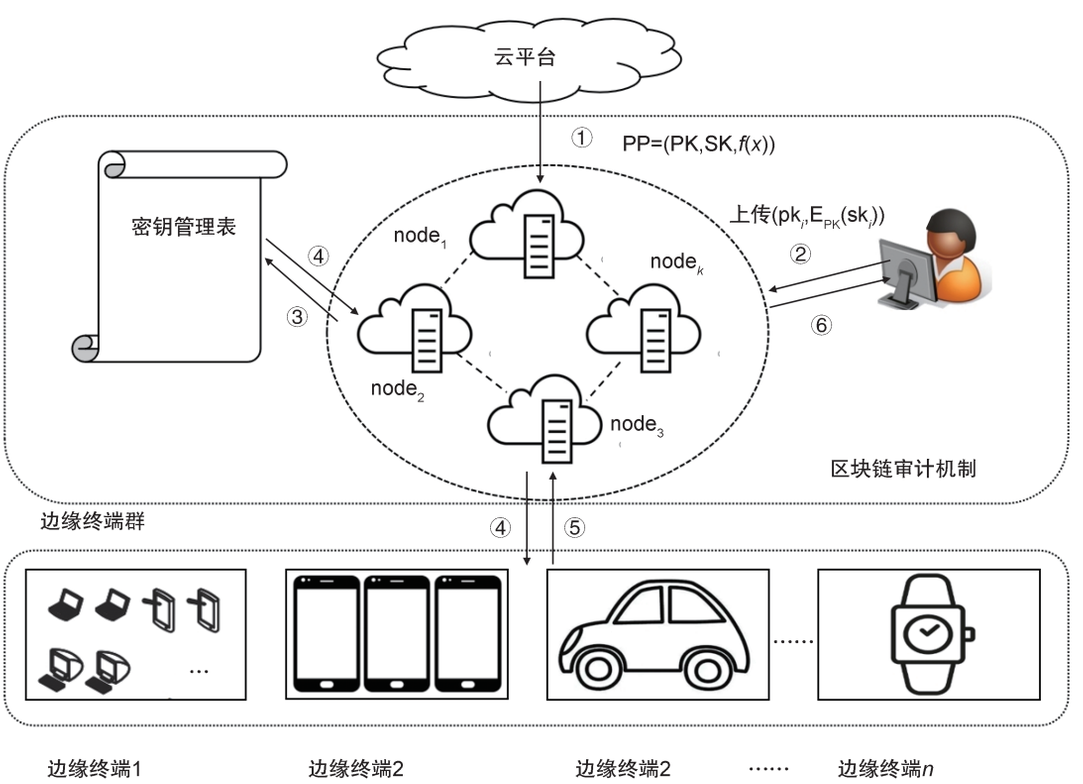
(3)计算需求用户:该用户会生成自己的密钥对(pk, sk),并使用全局公钥PK加密自身私钥得到E_{PK}(sk),最终上传密钥对(pk, E_{PK}(sk))至区块链(新隐私保护边缘计算架构中的用户可以采用任意同态加密算法)。

(4)密钥管理表:存储各边缘终端上传的上传密钥(pk, E_{PK}(sk))。在需要审计操作时,使用全局私钥SK解密获取边缘终端私钥sk。最终实现解密密文记录的目标。

(5)边缘终端:各终端节点在参与运算时可查询密钥管理表中的密钥对。其中终端节点包括计算终端和数据终端,计算终端提供算力支持,数据终端提供数据源。

2.1.2 系统模型的设计目标

新隐私保护边缘计算架构UPECA的设计目标是构建了一种用户管理机制完善、可自定义底层加密原语的去中心化隐私保护边缘计算架构。相关特性的定义为1)**用户管理机制:**区块链审计机制中定义了一密钥安全管理表,记录所有查询用户的密钥对。2)**中心化:**区块链构建了一套完整的协议机制就是只有当大部分节点或者多个关键节点认可数据的正确性时,



注:$node_k$为区块链节点,PP为云平台生成密钥对,$f(x)$为拉格朗日插值函数。① ② ③ ④ ⑤分别指进程j、k、l、m、n,⑥指计算后的返回值

图3 新隐私保护边缘计算架构UPECA的系统模型

Fig. 3 System model of the privacy-preserving edge computing architecture

数据才能被记入区块当中。3)**恶意用户可追溯**:区块链审计机制会存储各边缘终端上传计算记录。若出现非法数据或违规操作,该机制能够追溯对应恶意用户。4)**隐私性**:该架构能保障所有边缘终端数据的隐私性。5)**安全性**:新隐私保护边缘计算架构中所涉及的所有加密算法都基于数学困难问题,所有加密算法都满足选择明文攻击下的密文的不可区分性。

2.2 安全模型

2.2.1 敌手模型

定义1(敌手模型)在本文安全模型中存在一敌手A,该敌手A可能隐藏在区块链节点、用户和边缘终端中且具备以下威胁:

1)敌手A会试图收集和推测在工作期间接收到的数据复本。

2)若敌手A来自边缘终端群或用户,它可能尝试解密另一服务器的密文信息或提交非法数据集或非法skyline请求。

2.2.2 安全需求

新隐私保护边缘计算架构UPECA的安全目标是保护架构内所有边缘终端的数据隐私性。具体安全需求有:

1)**请求隐私性**:各边缘终端无法获取用户的明文信息。

2)**返回值的隐私性**:云平台、各边缘终端无法知悉查询结果的明文内容。仅用户可获取查询返回值的明文。

3)**边缘隐私性**:边缘终端的运算数据无法被获取。另外,新隐私保护边缘计算架构UPECA还需要防范恶意参与者。

3 隐私保护边缘计算架构UPECA

本节给出新隐私保护边缘计算架构UPECA的方案设计。同时本节对该方案进行理论分析,证明其对于任意PPT(Probabilistic Polynomial Time)敌手UPECA都是安全的。

3.1 UPECA架构的设计

本文设计目标是构建一种用户管理机制完善、可自定义底层加密原语的去中心化隐私保护边缘计算架构。如图4所示,对于某一计算请求方A,新隐私保护边缘计算架构UPECA主要包括以下6个工作进程:

(1)系统初始化:首先,架构执行ECC加密算法生成全局密钥对(PK, SK, $f(x)$),并采用Shamir秘密分割门限技术将SK分割为k个子密码(PK, SK_i, $f(x_i)$),发送至各区块链节点。选择一个$k-1$次多项式$f(x)$的k个互不相同的点的函数值$f(x_i)$($1 \leqslant i \leqslant k$),并构造多项式$f(x)$。具体地,

$$f(x)=\sum_{j=1}^{k}\phi(x_j)\prod_{l=1,l\neq j}^{k}\frac{(x-x_l)}{(x_j-x_l)}$$

设密钥SK $=f(0)$, k个子密钥取$f(x_i)$($1 \leqslant i \leqslant k$)。其次,计算请求方A生成密钥对($pk_a$, sk_a),并将(pk_a, $E_{PK}(sk_a)$)上传至密钥管理表。

(2)计算请求(进程j):计算请求方向UPECA架构发起计算请求Request。

(3)密钥获取(进程k):所有边缘终端节点都可以获取密钥管理表中的密钥对(pk_a, $E_{PK}(sk_a)$)。

(4)算力支持(进程l):计算节点向UPECA架构提供算力资源。

(5)数据支持(进程m):数据节点向UPECA架构提供符合要求的数据集。

(6)结果返回(进程n):UPECA架构返回计算结果Response。

此外,UPECA架构是基于区块链审计机制和密码学技术所构建的,其主要属性如下:

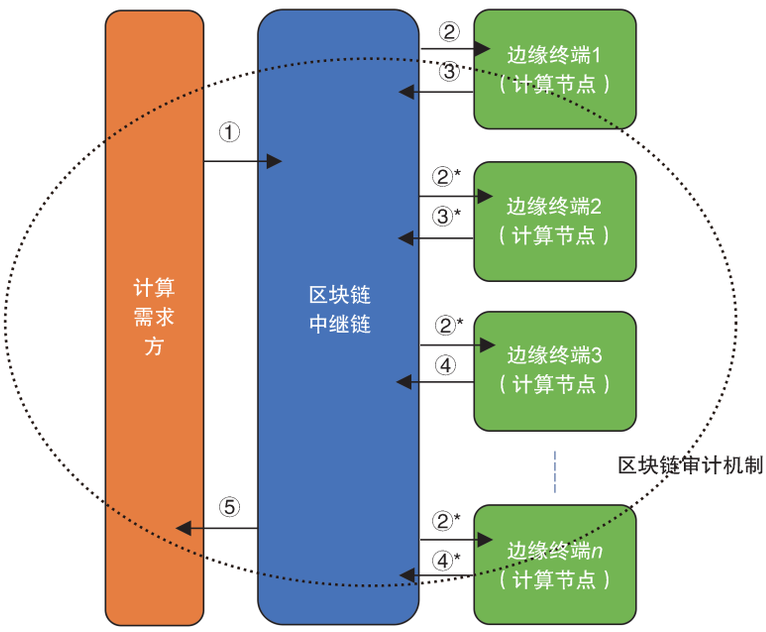
用户管理机制:UPECA架构的用户密钥都存储在区块链共同维护的密钥管理表中,提交计算的用户无法抹去自己操作痕迹。因此,系统可以追踪到各用户便于管理。

区块链审计:当UPECA架构发起审计操作时,各区块链维护节点使用Shamir秘密分割门限技术,对于任意k个用户汇聚其子密码后构造如下线性方程组

$$\begin{cases} f(x_1)=\mathrm{SK}+a_1\cdot x_1+a_2\cdot {x_1}^2+\cdots+a_{k-1}\cdot {x_1}^{k-1} \\ f(x_2)=\mathrm{SK}+a_1\cdot x_2+a_2\cdot {x_2}^2+\cdots+a_{k-1}\cdot {x_2}^{k-1} \\ \vdots \\ f(x_k)=\mathrm{SK}+a_1\cdot x_1+a_2\cdot {x_1}^2+\cdots+a_{k-1}\cdot {x_1}^{k-1} \end{cases}$$

可转换为矩阵方程

$$\begin{bmatrix} 1 & x_1^1 & x_1^2 & \cdots & x_1^{k-1} \\ 1 & x_2^1 & x_2^2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_k^1 & x_k^2 & \cdots & x_k^{k-1} \end{bmatrix}\cdot\begin{bmatrix} SK \\ a_1 \\ \vdots \\ a_{k-1} \end{bmatrix}=\begin{bmatrix} f(x_1) \\ f(x_2) \\ \vdots \\ f(x_{k-1}) \end{bmatrix}。$$



注:① ② ③ ④ ⑤分别指进程j、k、l、m、n;②和②*,③和③*,④和④*表示进程相同,传输的数据不同。

图4 新隐私保护边缘计算架构UPECA的工作进程

Fig. 4 Working process of the UPECA

最终通过解矩阵方程可得$f(0)$的值,从而获得全局私钥SK。然后架构访问密钥管理表中用户A的密钥对,在通过解密该私钥得到$sk_a = ECC.decrypt(E_{PK}(sk_a), SK)$。最后使用$sk_a$加密区块链中记录的所有操作事件,从而锁定边缘终端是否存在非法操作。

用户自定义:架构支持用户自定义底层加密原语。根据计算需求,架构可以自定义底层加密原语。

3.2 安全性证明

新隐私保护边缘计算架构UPECA的安全性主要涉及区块链的安全性和边缘终端的安全性。区块链的安全性证明已在文献[24]中给出,本节重点证明边缘终端的安全性。

定理1 对于任意多项式时间的敌手A,新隐私保护边缘计算架构UPECA中任意边缘终端都是安全的。

证明(定理1)设λ是一安全参数,$\sum$为新隐私保护边缘计算架构UPECA中所有边缘终端集合,S为一个多项式时间模拟器,A为PPT敌手,Π为底层加密算法。我们构建两个模拟视图Game1和Game2计算其输出在多项式时间内计算上不可区分。

Game 1:本模拟视图的执行环境是现实世界,其参与者包括挑战者CH和PPT敌手A。具体内容如下:

$Exp^{Game_1}_{Paillier,\ A}(\lambda)$

(pk,sk)←Paillier.keygen(λ); 请求方生成密钥对;

(pk,E_{PK}(sk))←Blockchain.query(); 敌手A获取

上传两个数据集$\{D_0, D_1\}$给CH;

D_b←$\{D_0, D_1\}$// CH随机选择一数据集

$E(D_b)$←Paillier.enc(D_b)

R←A.computer($\sum$,$E(D_b)$)//敌手A执行边缘计算

b^*←A.guess($\sum$,R, $E(D_b)$, pk, E_{PK}(sk))//敌手A猜测

若$b^* == b$则返回1,否则返回0。

视图Game1中,挑战者CH执行Paillier加密算法生成一密钥对(pk, sk)并上传(pk,E_{PK}(sk))至密钥管理表。敌手A查询密钥管理表获取(pk,E_{PK}(sk))后上传两个数据集$\{D_0, D_1\}$给CH。然后,挑战者CH从$\{D_0, D_1\}$中随机选择一数据集D_b用于实验。挑战者CH加密D_b后供敌手进行边缘计算获得结果R,并猜测是哪个数据集。若猜测正确返回1,否则返回0。

Game 2:本模拟视图的执行环境是理想世界。该视图存在一个多项式时间模拟器S,具备模拟任意加密数据集合P^*的能力。敌手A可以调用模拟器S的能力参与游戏的猜测挑战。此外我们还定义敌手A掌握了架构在信息

交互过程中的部分泄露ϵ。我们定义模拟视图Game2如下:

$\mathrm{Exp}^{\mathrm{Game_2}}_{\mathrm{Paillier,\ A}}(\lambda)$

(pk,sk)←Paillier.keygen(λ); 请求方生成密钥对;

(pk,E_{PK}(sk))←Blockchain.query(); 敌手A获取

上传两个数据集$\{D_0,D_1\}$给CH;

D_b←$\{D_0,D_1\}$ // CH随机选择一数据集

E(D_b)←Paillier.enc(D_b)

R←A.computer($\sum$,E(D_b))//敌手A执行边缘计算

b^*←A.guess($\sum$,R,ϵ, S, E(D_b), pk, E_{PK}(sk))//敌手A猜测

若 $b^*==b$ 则返回1,否则返回0;

模拟视图Game2的挑战过程与Game1的挑战过程相似。区别仅在于敌手A可以调用模拟器S的能力且掌握了边缘终端群$\sum$在传输数据过程中的部分泄露ϵ。这些能力对敌手A猜测b值可能存在优势。

分析可得,敌手A需要突破选择明文攻击下的密文的不可区分性,才具备攻击优势。敌手A在理想状态下的攻击优势可规约至敌手A攻破底层密码原语的优势,即敌手A在多项式时间内攻克判定n阶剩余类难题[25]。因此,在模拟视图Game 2下敌手A的所掌握的优势不高于在视图Game 1中的敌手,即

$$|\mathrm{Adv}^{\mathrm{Game\ 2}}_{\mathrm{Paillier,\ A}}-\mathrm{Adv}^{\mathrm{Game\ 1}}_{\mathrm{Paillier,\ A}}|=$$

$$|\Pr(\mathrm{Game2}(\lambda)=1)-\Pr(\mathrm{Game1}(\lambda)=1)|=\epsilon。$$

定理1得证。

4 性能分析

为了更真实地呈现新隐私保护边缘计算架构UPECA的性能特征,本节将分为两部分对其进行分析。一是结合分析Hyperledger fabric性能特征的经典文献[26-27],对新架构UPECA的交易开销进行分析。二是进行仿真模拟对UPECA架构的计算开销进行分析。

4.1 理论分析

本小节聚焦分析新架构UPECA的交易开销。根据Hyperledger fabric白皮书[28]定义,交易开销取决于系统架构平均吞吐量(每秒完成交易次数)的高低。具体地,Hyperledger fabric的平均吞吐量与版本、peer节点数、迭代次数、背书策略(Endorsement policy)都有直接影响。本文引用经典文献[26]中的分析结果,并绘制表1作出说明。此外,我们选取Paillier加密算法[29]、ElGamal加密算法[30]和CKKS全同态加密算法[31]作为底层加密技术进行分析。为了确保分析结果的有效性和可读性,本节固定各算法的密钥长度为512 bit(维度为8 192)。具体分析结果如下:

实验分析了新架构UPECA在背书策略为OR_{10}或AND_5状态下peer节点数依次递增时三种加密算法的交易开销变化。其中,我们定义边缘计算次数$n=1\ 000$。如图5所示,新架构的通信开销与其吞吐量成反比,即架构的平均吞吐量越大通信开销越小。这为提升隐私保护边缘计算架构的通信开销指明的研究方向。

表1 参数说明表

Table 1 Parameters description

参数名称	变化情况
版本号	Hyperledger fabric 1.4(固定值)
迭代次数	1次(固定值)
背书策略	OR_{10}、AND_5
peer节点数(个)	1、3、5、7(OR_{10}); 1、3、5(AND_5)
吞吐量(tps)	50、150、246、310(OR_{10});50、150、250(AND_5)
交易规模	1 byte
密文规模	128 byte(Paillier or ElGamal),131 072 byte(CKKS)

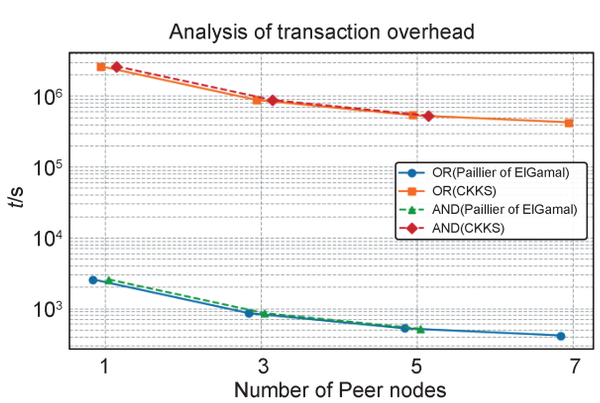


图5 交易开销分析图

Fig. 5 Analysis of transaction overhead

4.2 实验分析

由于新架构UPECA的交易操作和同态运算是异步执行,本小节仅聚焦分析新架构UPECA的计算开销(即同态运算开销)和通信开销。本文也选择对Paillier加密算法[29]、ElGamal加密算法[30]以及CKKS全同态加密算法[31]进行仿真实验。具体内容如下。

4.2.1 实验环境

本文实验将在 Windows 10 (Intel Core I5-8400 2.8 GHz)下搭建虚拟机(VMware workstation Pro 16)进行,区块链系统使用 Hyperledger fabric 1.4 构建,编程语言采用 python 3.8,具体如表 2 所示。此外,实验的数据集引用了 kaggle 平台上的两个真实数据集和一个随机(RND)数据集。真实数据集为 Online Retail (OR)数据集①和 Daraz Online Shopping (DOS)数据集②。该实验过程中数据是随机选择的,以满足实验的随机性。

表 2 实验环境

Table 2 Experimental configurations

实验环境	配置
操作系统	Windows 10
处理器	Intel Core I5-8400 2.8 GHz
内存	16 GB
虚拟机版本	VMware workstation Pro 16
区块链系统	Hyperledger fabric 1.4
编程语言	python 3.8
CKKS 算法库	Tenseal 0.3.14
ElGamal、Paillier 算法库	Pycryptodome 3.14.1

4.2.2 实验部署

系统搭建阶段,我们基于 Hyperledger Fabric 1.4 系统实现了区块链审计机制,部署包含 1 个 orderer 节点和 3 个 peer 节点作为区块链维护节点。然后,系统使用 Shamir 的秘密共享技术将云平台的全局私钥 SK 分割成若干份发送至各区块链节点,用于维护和审计操作。另外,架构采用 python3.8 代码构建套接字 socket 实现各端点的通信,这个通信节点用于模拟各边缘计算终端。边缘计算终端通过调用加密算法接口实现加密运算。最后,我们基于上述部署对新隐私保护边缘计算架构 UPECA 进行计算开销的分析,即同态运算的开销。

4.2.3 实验结果

实验分析了新架构 UPECA 在三种不同数据集下执行同态操作的计算开销变化。其中,我们定义边缘计算次数 $n = 1\,000 \sim 12\,000$。如图 6 所示,同态操作的计算开销与事件计算次数成正比,即事件计算次数越多同态操作的计算开销越大。

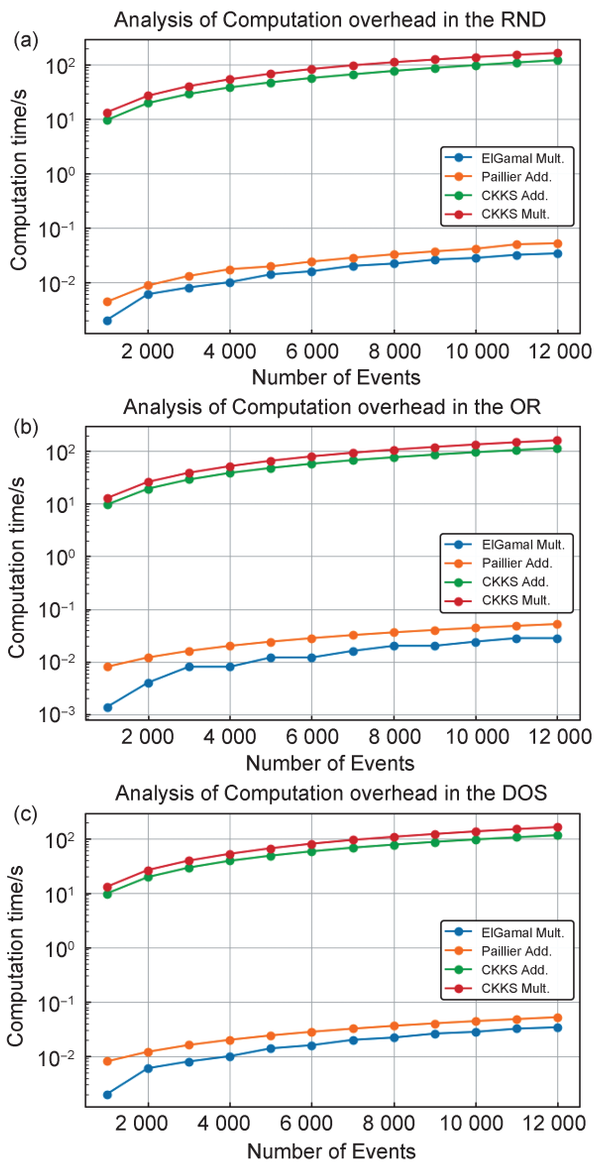


图 6 计算开销分析图

Fig. 6 Analysis of computational overhead

此外,架构采用 CKKS 加密算法执行同态加操作的平均计算开销约为 Paillier 加密算法的 1 960.76 倍,其执行同态乘操作的平均计算开销约为 ElGamal 加密算法的 4 771.65 倍。可见,全同态加密算法虽然具备抗量子攻击特性,但需要更多的计算开销。通过在不同数据集上进行仿真实验得出,不同的数据集不会影响同态操作的计算开销变化。

5 结论

本文设计了一种用户管理机制完善、可自

① https://www.kaggle.com/datasets/samantas2020/online-retail-xlsx

② https://www.kaggle.com/datasets/efazmahmudayon/graphics-card-price-in-daraz-for-july-2023

定义底层密码原语的可适用场景多类型应用场景的新隐私保护边缘计算架构。该架构不仅保障了边缘数据的计算隐私性,还实现了架构的自适用性。为了证实新隐私保护边缘计算架构的可行性及安全性,本文首先引入形式化安全证明的模型证明本文架构的安全性规约至底层密码原语。其次,本文选取了Paillier加密算法、ElGamal加密算法和CKKS加密算法在三种数据集上进行了仿真模拟。分析结果表明本文设计的新隐私保护边缘计算架构符合多场景的工业应用标准,且具有较高的实用性和安全性。

参考文献:

[1] KAHRAMAN İ, KÖSE A, KOCA M, *et al*. Age of Information in Internet of Things: a Survey[J]. *IEEE Internet Things J*, 2024, **11**(6): 9896−9914. DOI: 10.1109/JIOT.2023.3324879.

[2] AGYAPONG P K, IWAMURA M, STAEHLE D, *et al*. Design Considerations for a 5G Network Architecture[J]. *IEEE Commun Mag*, 2014, **52**(11): 65−75. DOI: 10.1109/MCOM.2014.6957145.

[3] 蔡睿, 葛军, 孙哲, 等. AI预训练大模型发展综述[J]. 小型微型计算机系统, 2024, **45**(10): 2327−2337. DOI: 10.20009/j.cnki.21−1106/TP.2023−0571.
CAI R, GE J, SUN Z, *et al*. Overview of Development of AI Pre−trained Large Model[J]. *J Chin Comput Sys*, 2024, **45**(10): 2327−2337. DOI: 10.20009/j. cnki. 21−1106/TP.2023−0571.

[4] KHAN W Z, AHMED E, HAKAK S, *et al*. Edge Computing: a Survey[J]. *Future Gener Comput Syst*, 2019, **97**: 219−235. DOI: 10.1016/j.future.2019.02.050.

[5] SATYANARAYANAN M. The Emergence of Edge Computing[J]. *Computer*, 2017, **50**(1): 30−39. DOI: 10.1109/MC.2017.9.

[6] LIU M T, YU F R, TENG Y L, *et al*. Distributed Resource Allocation in Blockchain-based Video Streaming Systems with Mobile Edge Computing[J]. *IEEE Trans Wirel Commun*, 2019, **18**(1): 695−708. DOI: 10.1109/TWC.2018.2885266.

[7] PACE P, ALOI G, GRAVINA R, *et al*. An Edge-based Architecture to Support Efficient Applications for Healthcare Industry 4.0[J]. *IEEE Trans Ind Inform*, 2019, **15**(1): 481−489. DOI: 10.1109/TII.2018.2843169.

[8] NGUYEN D C, PATHIRANA P N, DING M, *et al*. BEdgeHealth: a Decentralized Architecture for Edge-based IoMT Networks Using Blockchain[J]. *IEEE Internet Things J*, 2021, **8**(14): 11743−11757. DOI: 10.1109/JIOT.2021.3058953.

[9] SAYED A, HIMEUR Y, ALSALEMI A, *et al*. Intelligent Edge-based Recommender System for Internet of Energy Applications[J]. *IEEE Syst J*, 2022, **16**(3): 5001−5010. DOI: 10.1109/JSYST.2021.3124793.

[10] REHMAN M A U, SALAH UD DIN M, MASTORAKIS S, *et al*. FoggyEdge: an Information-centric Computation Offloading and Management Framework for Edge-based Vehicular Fog Computing [J]. *IEEE Intell Transp Syst Mag*, 2023, **15**(5): 78−90. DOI: 10.1109/MITS.2023.3268046.

[11] MENEGUETTE R, DE GRANDE R, UEYAMA J, *et al*. Vehicular Edge Computing: Architecture, Resource Management, Security, and Challenges[J]. *ACM Comput Surv*, 2023, **55**(1): 1−46. DOI: 10.1145/3485129.

[12] HUA H C, LI Y T, WANG T H, *et al*. Edge Computing with Artificial Intelligence: a Machine Learning Perspective[J]. *ACM Comput Surv*, 2023, **55**(9): 1−35. DOI: 10.1145/3555802.

[13] MCENROE P, WANG S, LIYANAGE M. A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges[J]. *IEEE Internet Things J*, 2022, **9**(17): 15435−15459. DOI: 10.1109/JIOT.2022.3176400.

[14] SHEIKHALISHAHI M, SARACINO A, MARTINELLI F, *et al*. Privacy Preserving Data Sharing and Analysis for Edge-based Architectures[J]. *Int J Inf Secur*, 2022, **21**(1): 79−101. DOI: 10.1007/s10207-021-00542-x.

[15] HE C R, LIU G Y, GUO S T, *et al*. Privacy-preserving and Low-latency Federated Learning in Edge Computing[J]. *IEEE Internet Things J*, 2022, **9**(20): 20149−20159. DOI: 10.1109/JIOT.2022.3171767.

[16] LIU B Y, LI Y C, LIU Y X, *et al*. PMC: A Privacy-preserving Deep Learning Model Customization Framework for Edge Computing[J]. *Proc ACM Interact Mob Wearable Ubiquitous Technol*, 2020, **4**(4): 1−25. DOI: 10.1145/3432208.

[17] JIANG B, LI J Q, WANG H H, *et al*. Privacy-preserving Federated Learning for Industrial Edge Computing via Hybrid Differential Privacy and Adaptive Compression[J]. *IEEE Trans Ind Inform*, 2023, **19**(2): 1136−1144. DOI: 10.1109/TII.2021.3131175.

[18] GU B, GAO L X, WANG X D, *et al*. Privacy on the Edge: Customizable Privacy-preserving Context Sharing in Hierarchical Edge Computing[J]. *IEEE Trans*

Netw Sci Eng, 2020, **7**(4): 2298−2309. DOI: 10.1109/TNSE.2019.2933639.

[19] BI M N, WANG Y J, CAI Z P, *et al*. A Privacy-preserving Mechanism Based on Local Differential Privacy in Edge Computing[J]. *China Commun*, 2020, **17**(9): 50−65. DOI: 10.23919/JCC.2020.09.005.

[20] ELHATTAB F, BOUCHENAK S, BOSCHER C. Pastel: Privacy-preserving federated learning in edge computing[J]. *Proc ACM Interact Mob Wearable Ubiquitous Technol*, 2023, **7**(4): 1−29. DOI: 10.1145/3633808.

[21] ZHANG R L, ZHOU R T, WANG Y F, *et al*. Incentive Mechanisms for Online Task Offloading with Privacy-preserving in UAV-assisted Mobile Edge Computing[J]. *IEEE/ACM Trans Netw*, 2024, **32**(3): 2646−2661. DOI: 10.1109/TNET.2024.3364141.

[22] MA Z F, WANG J Y, GAI K K, *et al*. Fully Homomorphic Encryption-based Privacy-preserving Scheme for Cross Edge Blockchain Network[J]. *J Syst Archit*, 2023, **134**: 102782. DOI: 10.1016/j.sysarc.2022.102782.

[23] ZENG S C, HSU C, HARN L, *et al*. Efficient and Privacy-preserving Skyline Queries over Encrypted Data Under a Blockchain-based Audit Architecture[J]. *IEEE Trans Knowl Data Eng*, 2024, **36**(9): 4603−4617. DOI: 10.1109/TKDE.2024.3373602.

[24] NAKAMOTO S. Bitcoin: a Peer-to-peer Electronic Cash System[J/OL]. *SSRN Journal*, 2008: 1−9. https://nakamotoinstitute.org/library/bitcoin/

[25] PAPADIMITRIOU C H. Computational Complexity [M]//Encyclopedia of Computer Science. Untied Kingdom: John Wiley and Sons Ltd., 2003: 260−265. DOI: 10.5555/1074100.1074233.

[26] WANG C H, CHU X W. Performance Characterization and Bottleneck Analysis of Hyperledger Fabric[C]//2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). New York: IEEE, 2020: 1281−1286. DOI: 10.1109/ICDCS47774.2020.00165.

[27] CAPOCASALE V, GOTTA D, PERBOLI G. Comparative Analysis of Permissioned Blockchain Frameworks for Industrial Applications[J]. *Blockchain Res Appl*, 2023, **4**(1): 100113. DOI: 10.1016/j.bcra.2022.100113.

[28] ANDROULAKI E, BARGER A, BORTNIKOV V, *et al*. Hyperledger Fabric: a Distributed Operating System for Permissioned Blockchains[C]//Proceedings of the Thirteenth EuroSys Conference. New York: ACM, 2018: 30. DOI: 10.1145/3190508.3190538.

[29] PAILLIER P. Public-key Cryptosystems Based on Composite Degree Residuosity Classes[M]//Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999: 223−238. DOI: 10.1007/3-540-48910-x_16.

[30] ELGAMAL T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms[J]. *IEEE Trans Inf Theory*, 1985, **31**(4): 469−472. DOI: 10.1109/TIT.1985.1057074.

[31] CHEON J H, KIM A, KIM M, *et al*. Homomorphic Encryption for Arithmetic of Approximate Numbers[C]//International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer, 2017: 409−437.10.1007/978−3−319−70694−8_15.